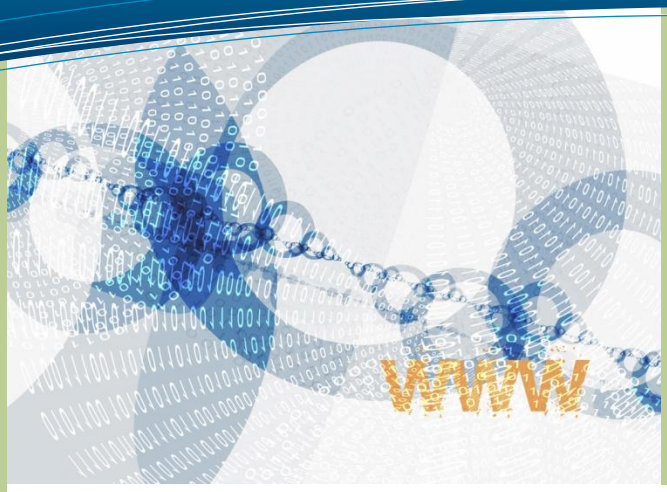
February 2010

MONTHLY Cyber Security Newsletter

Security Tips



Mississippi Department of Information Technology Services

Division of Information Security

This issue…

This month's newsletter provides you with information regarding backing up your data.

Remember…

Even a secure computer can fail, causing you to lose all of your data. If you follow a few simple tips and make it a habit to regularly back up all critical information on your computer, you can protect yourself from computer disasters.

How Important is Backing Up Your Data and Testing Those Backups?

According to Kabooza-2009 Global Survey, more than 80% of computer users surveyed do not back up their home PC regularly, and 50% do not back it up at all. Developing a backup and recovery plan for data residing on your computer is an important step every computer user and organization should take.

Loss of data can be devastating, especially if the information cannot be recovered or reproduced. Whether data is lost due to a physical disaster, virus, theft, or accidental deletion, the recovery of the data cannot be accomplished unless you have a plan in place. The need to back up important data to ensure its availability in the event of loss or theft cannot be overstated. Backup and recovery plans are essential not only for government and businesses but also for home users.

What Should You Backup?

All critical files, as well as any information not easily replaceable should be backed up. This could include business records and financial data, emails, address book and calendars, and any other information that has value to the individual or organization.

How Do You Backup Your Data?

- **Use your computer's backup tools.** Most operating systems now provide backup software designed to make the process easier.
- **Backup data at regular intervals**. Evaluate the importance of your data and the frequency of change in the data to determine the necessary frequency with which the data should be backed up.
- **Verify the data has been backed up.** Backup media needs to be reviewed periodically to determine if all of the data has been backed up accurately. Use the "backup log" provided by most backup applications. Generate a "backup report" that can quickly identify problems or skipped files. Be sure to review these logs periodically.

this newsletter is brought to you by…

www.msisac.org

www.its.ms.gov/services_security.shtml

- **Store the backup media in a secure location.** It is recommended that two backups be maintained: one on-site and one off-site. Backup media should be stored in a physically secure location.
- **Verify the ability to restore.** It is a best practice to periodically test that your backup data can be restored if loss occurs.
- **USB Flash drives**, sometimes called "thumb" drives, typically have limited storage and may not be practical for storing large amounts of data.
- **CDs** offer more storage capacity than flash drives but can be slow in copying and retrieving files. They're useful for home users with llimited amounts of data to back up.
- **DVDs** provide much greater storage capacity than CDs.
- **External Hard drives** are very effective backup devices. They typically have large storage capacity, and allow for extremely rapid copying of files and recovery of stored files.
- **Tapes** are commonly used in government and businesses where large amounts of data need to be backed up on a regular basis.
- **Online backup services** offer varying levels of storage and recovery options that can be tailored based on needs.

Note: *Many organizations have formal processes to backing up systems and no action by the end user is required.*

For additional information, please visit:

- **MS-ISAC Guidelines for Backing Up Information – A Non-Technical Guide**
  http://www.msisac.org/awareness/documents/Backing-Up-Information-Guide.pdf
- **Microsoft backup procedures for various Operating Systems**
  http://www.microsoft.com/protect/data/backup/about.aspx
- **StaySafeOnline**
  http://www.staysafeonline.org/content/back-up-your-files-and-data

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. Organizations have permission--and in fact are encouraged--to redistribute this newsletter in whole for educational, non-commercial purposes.